

Administrative sanctions will be imposed against those who violate LGPD

Failure to observe the law may result in loss of investments and business opportunities, damage to reputation and many other losses.

SãO PAULO, SãO PAULO, BRAZIL, May 8, 2023 /EINPresswire.com/ -- If, a while ago, there were no reasons to postpone works on adjusting personal data processing activities to the Brazilian General Data Protection Law (LGPD), it now seems that the pressure is building up after Resolution No. 4 of the Brazilian Data Protection Authority (ANPD) has been published – step that was missing for the authority to impose administrative penalties against those who break the law.

Ever since the LGPD was published in 2018, companies have given many reasons for not prioritizing compliance with the law. At the beginning, their argument was that this would be premature, as the law would only come into force a while later, and agents had been given a deadline to take the necessary measures to comply with all the new obligations.

When, in September 2020, the law took effect almost in its entirety, except for the articles about administrative sanctions, which would only come into force in the following year, the arguments for postponing compliance were also based on the very incipient structure of ANPD, the body responsible for imposing the sanctions provided for in the LGPD. At the time, we were in a whirlwind of emotions with the rapid spread of coronavirus, and companies had to fully change their ways of working, find out answers to the new questions that arose, and prioritize several actions unrelated to the LGPD.

Arguments became even stronger with the long discussion on the effective date of the articles regarding the penalties, which was even humorously compared to TV series Dark, known for generating debates about timelines. Originally, the articles regarding sanctions would come into effect 18 months after the official publication. However, Laws No. 13,853/2019 and 14,010/2020 and Provisional Presidential Decree No. 959/2020 (converted into Law No. 14,058/2020) kept pushing back the date such articles would come into force. This back-and-forth of dates was only solved in June 2020, when August 1st, 2021 was set as the effective date.

After this discussion, the reason for postponing compliance then became ANPD lack of regulation on sanctioning processes, an argument often presented in the year of 2020, during which a public hearing was held to discuss the topic, and a public inquiry received over 2,500

inputs from different segments of the civil society, the legal sector, the academia, and the industry.

Today, with the pandemic under control, a well-structured authority that has excellent professionals and is now ready to inspect and sanction all of those who violate the LGPD, there seems to be no more room for “excuses.” The recently published new resolution establishes criteria for ANPD to impose administrative sanctions and defines how to calculate the base value of fine sanctions. The seriousness of violations is classified into three levels – mild, medium, and serious – and the mitigating and aggravating circumstances to be considered in the final calculation of the fine are also presented.

The possible sanctions under the LGPD include issuing warnings, suspending the use of affected personal databases, making violations public, imposing fines, with a total limit of BRL 50 million per violation, and partially or fully suspending activities related to data processing.

According to public information released by ANPD, at least eight administrative processes are already pending trial, which, although confidential, indicate that the first decisions may be rendered in the first half of 2023.

Common violations against the LGPD that are subject to penalty include: information security incidents (such as recurrent data leaks), storage of unnecessary personal data, failure to comply with individuals’ requests related to the use of their personal data (such as access, correction, deletion, etc.), use of personal data for purposes other than those expected by data subjects, and discrimination based on the misuse of personal data.

It is also important to highlight that sanctions will be imposed from now on, but they may relate to violations against the LGPD that have occurred since the law came into force and that are being investigated by ANPD in administrative proceedings already in progress (article 28 of CD/ANPD Resolution No. 4/2023). Thus, those who waited to comply with the law only when the sanctions could be imposed may not have adopted the best strategy.

In any case, now is always an excellent time to start. It is recommended that companies which are still far behind in their compliance efforts urgently assess their personal data processing activities to uncover any vulnerabilities and define a strategy to adopt measures to comply with the LGPD, either to avoid future lawsuits or mitigate any possible penalties (items II and III of article 13 of CD/ANPD Resolution No. 4/2023).

Among many other actions, it is essential to have an effective privacy policy for employees and customers, so that there is total transparency about how their personal data are processed; to strengthen systems and mechanisms that ensure information security; to conduct training sessions so that all the staff are aware of what they should and should not do in order to comply with the law; to enter into agreements with strong data protection clauses when personal data is shared between the parties; to hire an officer responsible for processing personal data where

required by regulation; and to adopt tools to control and manage requests from data subjects exercising their rights under the LGPD.

The fact that ANPD can now impose sanctions is another milestone in the history of Data Protection in Brazil and, possibly, the element that was missing for the companies' interest in effectively complying with the LGPD. However, it is always important to highlight that any hassle generated by non-compliance could be much more serious than a penalty, which, according to ANPD, is not the priority of its work. Failure to observe the law may result in loss of investments and business opportunities, damage to reputation, mistrust from consumers, suspension of activities (such as in the recurrent cases of ransomware attacks) and many other losses.

In this scenario: "better safe than sorry," as the saying goes. Doing what is right from the start will always be a huge advantage.

* [Luiza Sato](#) e [Bruna Borghi](#) Tomé are partners in the Cybersecurity & Data Privacy area at [TozziniFreire Advogados](#)

Natália Zulzke de Carvalho
TozziniFreire Advogados
+55 11 5086-5000

[email us here](#)

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

[Other](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/632463274>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.